



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

5e

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,088	12/11/2000	David Michael Kurn	20206-032 (P00-3016)	5327

7590 05/16/2005

Hewlett-Packard Company  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
----------	--------------

2133

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/735,088	<b>Applicant(s)</b> KURN ET AL.	
	<b>Examiner</b> Nadia Khoshnoodi	<b>Art Unit</b> 2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 12/27/2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-14 and 16-69 is/are pending in the application.
- 4a) Of the above claim(s) 15 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 and 16-69 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Response to Amendment*

Claim 15 has been cancelled. Amendments to the specification filed on December 27, 2004 have been accepted. Applicant's arguments/ amendments with respect to amended claims 1-14, 16-48, 50-53, 55-60, 66-69 and previously presented claims 49, 54, 61-65 filed December 27, 2004 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

### *Claim Rejections - 35 USC § 102*

I. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

II. Claims 1-11, 32, 35-49, 51-52, 62-63, and 65 are rejected under 35 U.S.C. 102(e) as being anticipated by Thomlinson et al., United States Patent No. 6,532,542.

As per claim 1:

Thomlinson et al. teach a computer system, said comprising: a server (col. 5, lines 38-50); a database comprising data and responsive to signals from said server (col. 6, lines 32-44); a key repository process executing on said server and comprising a master key used by said key repository process to protect data (col. 10, lines 18-42); and an application program executing on said server (col. 6, lines 32-35); wherein said key repository process stores and retrieves

Art Unit: 2133

authorization information maintained in said database, said authorization information used to determine if said applications program is authorized to access said data (col. 6, lines 41-67); and wherein said key repository process prevents access to said data by said application program if said application program is not authorized (col. 8, lines 36-46).

As per claim 2:

Thomlinson et al. further teach the computer system as in claim 1, wherein said key repository process uses said master key to decrypt said data (col. 10, lines 18-42).

As per claim 3:

Thomlinson et al. further teach the computer system as in claim 1, wherein said repository process uses said master key to encrypt said data (col. 10, lines 18-42).

As per claim 4:

Thomlinson et al. further teach the computer system as in claim 1, wherein said data comprises a public key (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 5:

Thomlinson et al. further teach the computer system as in claim 1, wherein said data comprises a secret (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 6:

Thomlinson et al. further teach the computer system as in claim 1, wherein said data comprises a private key (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 7:

Thomlinson et al. further teach the computer system as in claim 1, wherein said data comprises a symmetric key (col. 10, lines 27-50).

Art Unit: 2133

As per claim 8:

Thomlinson et al. further teach the computer system as in claim 1, wherein said data comprises a certification authority certificate (col. 8, line 25 – col. 9, line 8).

As per claim 9:

Thomlinson et al. further teach the computer system as in claim 1, wherein said master key is maintained in physical memory (col. 11, lines 7-13).

As per claim 10:

Thomlinson et al. further teach the computer system as in claim 1, wherein said master key is maintained in non-swappable physical memory (col. 11, lines 35-60).

As per claim 11:

Thomlinson et al. further teach the computer system as in claim 10, wherein said non-swappable physical memory is protected (col. 11, lines 35-60).

As per claim 32:

Thomlinson et al. teach the computer method comprising a server (col. 5, lines 38-50); a database comprising data, said database responsive to signals from said server (col. 6, lines 32-44); an application process executing on said server (col. 6, lines 32-35), said key repository process having a master key, said master key being used by said key repository process to protect said data (col. 10, lines 18-42); wherein said key repository maintains in said database the identity of those application processes authorized to access said data (col. 6, lines 41-67); and wherein if said application process is authorized to access said data, then said key repository process transmits said data to said application process (col. 8, lines 36-66).

As per claim 35:

Art Unit: 2133

Thomlinson et al. further teach the computer method as in claims 32, wherein said master key protects said data from modification (col. 10, lines 35-42).

As per claim 36:

Thomlinson et al. further teach the method as in claim 32, wherein said master key provides privacy protection to said data (col. 10, lines 18-42).

As per claim 37:

Thomlinson et al. further teach the method as in claim 32, wherein said data comprise a public key (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 38:

Thomlinson et al. further teach the method as in claim 32, wherein said data comprise a private key (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 39:

Thomlinson et al. further teach the method as in claim 32, wherein said data comprise a symmetric key (col. 10, lines 27-50).

As per claim 40:

Thomlinson et al. further teach the method as in claim 32, wherein said data comprise a trust root (col. 8, line 36 – col. 9, line 3).

As per claim 41:

Thomlinson et al. further teach the method as in claim 40, wherein said trust root comprises a digital fingerprint (col. 8, lines 25-46). Although the term “digital fingerprint” is not used, a certificate comprises of the digital signature of the trust root which is identical to that of a digital fingerprint.

Art Unit: 2133

As per claim 47:

Thomlinson et al. further teach the method as in claims 32, wherein said master key is kept in physical memory (col. 11, lines 7-13).

As per claim 48:

Thomlinson et al. further teach the method as in claim 32, wherein said master key is kept in non-swappable physical memory (col. 11, lines 35-60).

As per claim 49:

Thomlinson et al. further teach the method as in claim 48, wherein said non-swappable physical memory is protected (col. 1, lines 35-60).

As per claim 42:

Thomlinson et al. further teach the method of claim 32, wherein said data comprises a digital signature (col. 8, lines 25-35).

As per claim 43:

Thomlinson et al. further teach the method of claim 32, wherein said data comprises a digital certificate (col. 8, lines 25-35).

As per claim 44:

Thomlinson et al further teach the method of claim 32, wherein said data comprises a checksum (col. 8, lines 25-57). Although the term “checksum” is not used, the concept of what a checksum is used for is addressed by taking the binary hash and storing it so that in the future the hash can be used in order to determine whether or not any modifications occurred in the requesting program’s authentication information.

As per claim 45:

Art Unit: 2133

Thomlinson et al. further teach the method of claim 32, wherein said data comprises a hash (col. 8, line 63 – col. 9, line 4).

As per claim 46:

Thomlinson et al. further teach the method of claim 32, wherein said data comprises a characteristic code sequence (col. 11, lines 1-6).

As per claim 51:

Thomlinson et al. further teach the method of claim 32, wherein said master key comprises an integrity key being constructed and arranged to ensure the integrity of said data (col. 10, lines 35-42). Although the term integrity key is not used, a key authentication code is derived in order to verify the item key and ensure that it is decrypted to yield the same data that existed before the encryption process.

As per claim 52:

Thomlinson et al. further teach the method of claim 32, wherein said master key comprises a protection key, said protection key being constructed and arranged to protect said data (col. 10, lines 35-42).

As per claim 62:

Thomlinson et al. further teach the method of claim 32, wherein said authorization information includes a file location (col. 9, lines 1-8).

As per claim 63:

Thomlinson et al. further teach the method of claim 32, wherein said authorization information includes a physical address (col. 12, lines 20-28).

As per claim 65:



Art Unit: 2133

Thomlinson et al further teach the method of claim 32, wherein said authorization information includes a system residence (col. 11, lines 35-60).

***Claim Rejections - 35 USC § 103***

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

IV. Claims 12, 31, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al., United States Patent No. 6,532,542, as applied to claim 1 above, and further in view of Denning, *Virtual Memory*.

As per claims 12, 31, and 50:

Thomlinson et al. substantially teach the computer systems/method as in claims 1, 16, and 32. Furthermore, Thomlinson et al. teach storing the master key (col. 11, lines 7-13). Not explicitly disclosed by Thomlinson et al. is the computer system, wherein said master key is maintained in virtual memory. However, Denning teaches different advantages gained by using virtual memory. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer system/method disclosed in Thomlinson et al. to store the master key in virtual memory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Denning on page 216.

Art Unit: 2133

V. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al., United States Patent No. 6,532,542, as applied to claim 1 above and further in view of Menezes et al., *Handbook of Applied Cryptography*.

As per claim 13:

Thomlinson et al. substantially teach the computer system as in claim 1. Furthermore, Thomlinson et al. teach the computer system, wherein said master key is used to decrypt a key maintained in said database; and wherein said key is used to encrypt said data (col. 10, lines 28-42). Furthermore, Thomlinson et al. teach that both symmetric and asymmetric algorithms are well known for use in encryption/decryption in col. 3, lines 23-65. Not explicitly disclosed by Thomlinson et al. is the computer system, wherein the key is a public key. However, Menezes et al. teach that using public key cryptography has many advantages. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer system disclosed in Thomlinson et al. for the master key to decrypt a public key, which is used to encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Menezes et al. on page 31.

As per claim 14:

Thomlinson et al. substantially teach the computer system as in claim 13. Furthermore, Thomlinson et al. teach that both symmetric and asymmetric algorithms are well known for use in encryption/decryption in col. 3, lines 23-65. Not explicitly disclosed by Thomlinson et al. is the computer system, wherein the key is a public key. However, Menezes et al. teach that using public key cryptography has many advantages. Therefore, it would have been obvious to a

Art Unit: 2133

person in the art at the time the invention was made to modify the computer system disclosed in Thomlinson et al. for there to exist a master key and second master key, i.e. a public/private key pair used to encrypt/decrypt the public key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Menezes et al. on page 31.

VI. Claims 16-30, 33-34, 53-61, 64, and 66-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al., United States Patent No. 6,532,542.

As per claim 16:

A computer system comprising a server (col. 5, lines 38-50); a database comprising enterprise credentials, said database responsive to signals from said server (col. 6, lines 32-44 and col. 8, line 58 – col. 9, line 8); an application process executing on said server (col. 6, lines 32-35), said key repository process having a master key, said master key being used by said key repository process to protect said enterprise credentials (col. 10, lines 18-42 and col. 8, line 58 – col. 9, line 8); and wherein said key repository maintains in said database the identity of those application processes authorized to access said enterprise credentials (col. 6, lines 41-67 and col. 8, line 58 – col. 9, line 8).

Not explicitly disclosed by Thomlinson et al. is the computer method wherein if said application process is authorized to access said enterprise credentials, then said key repository process transmits said enterprise credentials to said application process (col. 8, lines 36-66). However, Thomlinson et al. teach that data items are transmitted only those who are authorized. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Thomlinson et al. for the term “data item” to refer also to the

Art Unit: 2133

“enterprise credentials” which are included in the data items stored in the database. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 7, line 49-53.

As per claim 17:

Thomlinson et al. further teach the computer system as in claims 16, wherein said master key protects said enterprise credentials from modification (col. 10, lines 35-42).

As per claim 18:

Thomlinson et al. further teach the computer system as in claim 16, wherein said master key provides privacy protection to said enterprise credentials (col. 10, lines 35-42).

As per claim 19:

Thomlinson et al. substantially teach the computer system as in claim 16. Not explicitly disclosed by Thomlinson et al. is the computer system wherein the master key protects said enterprise credentials from unauthorized deletion. However, Thomlinson et al. teach that access to the enterprise credentials is not granted unless the application program has been authorized. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Thomlinson et al. for the master key to protect the enterprise credentials from unauthorized deletion. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 11, lines 7-25.

As per claim 20:

Thomlinson et al. further teach the computer system/method as in claim 16, wherein said enterprise credentials comprise a public key (col. 7, lines 45-60 and col. 8, lines 25-35).

As per claim 21:

Thomlinson et al. further teach the computer system as in claim 16, wherein said enterprise credentials comprise a private key (col. 7, lines 45-60 and col. 8, lines 22-35).

As per claim 22:

Thomlinson et al. further teach the computer system as in claim 16, wherein said enterprise credentials comprise a symmetric key (col. 10, lines 27-50).

As per claim 23:

Thomlinson et al. further teach the computer system as in claim 16, wherein said enterprise credentials comprise a trust root (col. 8, line 36 – col. 9, line 3).

As per claim 24:

Thomlinson et al. further teach the computer system as in claim 23, wherein said trust root comprises a digital fingerprint (col. 8, lines 25-46). Although the term “digital fingerprint” is not used, a certificate comprises of the digital signature of the trust root which is identical to that of a digital fingerprint.

As per claim 25:

Thomlinson et al. further teach the computer system as in claim 23, wherein said trust root comprises a checksum (col. 8, lines 25-57). Although the term “checksum” is not used, the concept of what a checksum is used for is addressed by taking the binary hash and storing it so that in the future the hash can be used in order to determine whether or not any modifications occurred in the requesting program’s authentication information.

Art Unit: 2133

As per claim 26:

Thomlinson et al. further teach the computer system as in claim 23, wherein said trust root comprises a hash (col. 8, line 63 – col. 9, line 4).

As per claim 27:

Thomlinson et al. further teach the computer system as in claim 23, wherein said trust root comprises a cryptographic mechanism (col. 8, lines 28-35).

As per claim 28:

Thomlinson et al. further teach the computer system as in claim 16, wherein said master key is kept in physical memory (col. 11, lines 7-13).

As per claim 29:

Thomlinson et al. further teach the computer system as in claim 16, wherein said master key is kept in non-swappable physical memory (col. 11, lines 35-60).

As per claims 30:

Thomlinson et al. further teach the computer system as in claim 16, wherein said non-swappable physical memory is protected (col. 11, lines 35-60).

As per claim 33:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method, further comprising directing said key repository process to recognize an instance of said application program before querying said repository process. However, Thomlinson et al. teach that the application program must identify itself to the server first. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Thomlinson et al. for the key repository process to

Art Unit: 2133

recognize an instance of the application program before querying the repository process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 12, lines 6-20.

As per claim 34:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson is the method wherein said key repository process is constructed and arranged to record said authorization information in said database. However, Thomlinson et al. teaches storing authorization information in the database. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to also construct and arranged to record the authorization information in the database so that the data is organized. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 11, lines 7-25.

As per claim 53:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by use of a cryptographic technique (col. 12, lines 36-48).

As per claim 54:

Thomlinson et al. further teach the method of claim 53, wherein said cryptographic technique is a checksum (col. 12, lines 36-48). Although the term "checksum" is not used, the concept of what a checksum is used for is addressed by taking the binary hash and storing it so

Art Unit: 2133

that in the future the hash can be used in order to determine whether or not any modifications occurred in the requesting program's authentication information.

As per claim 55:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by its file location (col. 12, lines 60-67).

As per claim 56:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by its physical address (col. 12, lines 20-28).

As per claim 57:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by the system on which it is instantiated (col. 11, lines 35-66).

As per claim 58:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by the nature of the interconnection to said key repository (col. 12, lines 60-67).

As per claim 59:

Thomlinson et al. substantially teach the method of claim 33. Not explicitly disclosed by Thomlinson et al. is the method wherein said instance of said application program is recognized by its communication protocol. However, Thomlinson et al. teach that the application program can be sent over a network. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to identify the protocol used for the communication in order to recognize the packet. This



Art Unit: 2133

modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 4, lines 31-50.

As per claim 60:

Thomlinson et al. further teach the method of claim 33, wherein said instance of said application program is recognized by a packet header (col. 13, lines 1-4).

As per claim 61:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method wherein said authorization information includes a time constraint. However, Thomlinson et al. teach that the authorization information could include the date and time of the last time the program was saved or modified. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to use the time and date of when the program was last saved or modified in order to derive time constraints that could be used as authorization information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 9, lines 1-8.

As per claim 64:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method wherein said authorization information includes a universal resource locator. However, Thomlinson et al. teach that each system server is has various modules hard-coded with a public key in order to prevent tampering with the storage server.

Art Unit: 2133

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to have the authorization information include a universal resource locator to keep track of the storage systems. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 11, lines 35-60.

As per claim 66:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method, wherein said authorization information is initiated by an operator. However, Thomlinson et al. teach that a user can set up access privileges in such a way that they can physically grant access or deny access thereby having an operator initiate the authorization. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to have the authorization information initiated by an operator. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 9, lines 41-46.

As per claim 67:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method, wherein said authorization information is initiated by an owner. However, Thomlinson et al. teach that the authorization information is initiated by the server following a request from the client. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et

Art Unit: 2133

al. to have the authorization information initiated by an owner. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 12, lines 6-15.

As per claim 68:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method, wherein said authorization information is initiated by two or more owners. However, Thomlinson et al. teach that the authorization information is initiated by several modules in the server following a request from the client. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to have the authorization information initiated by two or more owners. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 12, lines 6-15.

As per claim 69:

Thomlinson et al. substantially teach the method of claim 32. Not explicitly disclosed by Thomlinson et al. is the method, wherein said authorization information is initiated by two or more owners. However, Thomlinson et al. teach that the authorization information is initiated by several modules in the server following a request from the client. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to have the authorization information initiated by two or more owners. This modification would have been obvious because a person having ordinary skill in

Art Unit: 2133

the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 12, lines 6-15.

Also not explicitly disclosed by Thomlinson et al. is the method wherein said authorization information is initiated by two or more owners and an operator. However, Thomlinson et al. teach that a user can set up access privileges in such a way that they can physically grant access or deny access thereby having an operator initiate the authorization. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the computer method disclosed in Thomlinson et al. to have the authorization information initiated by an operator. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Thomlinson et al. in col. 9, lines 41-46.

### *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

Art Unit: 2133

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825.

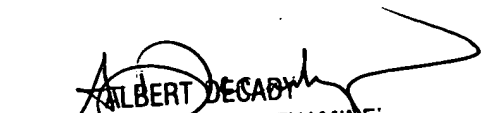
The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Nadia Khoshnoodi  
Examiner  
Art Unit 2133  
5/5/2005

NK



ALBERT DECADY  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 210